Information
and Privacy
Commissioner/
Ontario

Guidelines for Using Video Surveillance Cameras in Schools

Ann Cavoukian, Ph.D.
Commissioner
December 2003

Commissioner Ann Cavoukian gratefully acknowledges the work of Mark Ratner and Judith Hoffman, of the IPC's Policy and Compliance Department, in the preparation of this report.

She would also like to thank the British Columbia School Trustees Association and all of the Ontario school boards that contributed to the consultation process.

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

This publication is also available on the IPC Web site.
Cette publication est également disponible en français.

Table of Contents

Introduction 1

Applicability of the *Guidelines* 3

Definitions 4

Collection of Personal Information Using Video Surveillance 5

How to Decide Whether to Use a Video Surveillance System 6

Developing the Board Policy for Video Surveillance 7

Designing, Installing and Maintaining Video Surveillance Equipment 9

Procedures Governing the Use, Disclosure, Retention, Security and Disposal of Video Surveillance Records 11

Access to Personal Information 13

Auditing and Evaluating the Use of Video Surveillance 14

Other Resources 15

Appendix A – Covert Surveillance 16

Introduction

Increasingly, school boards in Ontario are using closed circuit television cameras as a means of monitoring school property. While the rationale underlying these closed-circuit systems varies, video surveillance is generally viewed as being useful in accomplishing three main goals: (1) enhancing the safety of students and staff, (2) protecting school property against theft or vandalism and (3) aiding in the identification of intruders and of persons breaking the law.

Municipal school boards in Ontario are subject to the *Municipal Freedom of Information and Protection of Privacy Act*, (the municipal *Act*). This *Act* imposes obligations on institutions with respect to the collection, use, disclosure, retention, security and disposal of personal information. Similarly, provincial schools in Ontario that are operated directly by the Ministry of Education are subject to the *Freedom of Information and Protection of Privacy Act* (the provincial *Act*). Largely, these two *Acts* are similar in terms of the obligations they impose on institutions with respect to the protection of the privacy interests of individuals.

By virtue of the definition of "institution" contained in both *Acts*, all public and separate school boards in the province are obliged to protect the personal privacy of individuals, in accordance with the legislation. The *Acts* provide rules to be followed by schools and school boards in the collection, use, accuracy, disclosure, safekeeping, retention and disposal of personal information.

In October 2001, the IPC issued its *Guidelines for Using Video Surveillance Cameras in Public Places*[1] to assist government organizations that had implemented or were in the process of implementing surveillance programs to ensure the programs complied with the privacy provisions of the *Acts*. This publication was specifically aimed at the video surveillance of public places and was not intended to address the privacy concerns that arise in the case of buildings, such as schools. The IPC has issued this paper, *Guidelines for Using Video Surveillance Cameras in Schools* (the *Guidelines*), to specifically address the school setting.

While these *Guidelines* retain the basic structure of, and express principles similar to, those enunciated in the original paper, these *Guidelines* recognize that modified expectations of privacy exist in schools. In contrast to public places, schools are considered to be a supervised environment where a reasonable degree of monitoring by school staff is both desirable and expected. A comprehensive surveillance system in a school, however, has the potential of being privacy-invasive. These *Guidelines* were created to assist school boards intending to use video surveillance to introduce these programs in a manner that ensures stringent privacy controls.

[1] www.ipc.on.ca/docs/video-e.pdf.

The IPC recommends that all school boards using video surveillance implement formal policies governing their use. In addition to helping boards fulfil their obligations under the *Acts*, the codification of a formal policy is an effective way to deal with any questions or concerns that may be raised by the public, including those of students and parents, as a result of the introduction of video cameras in board schools.

In addition to the adoption of formal policies at the board level, the IPC recommends that each school with a program in place have a set of written procedures that address day-to-day usage of the system. Minimum standards for the procedures should be expressed by the school board in the policy, or in the procedures themselves. The appropriate content for both the policies and procedures are dealt with in these *Guidelines*.

Applicability of the *Guidelines*

These *Guidelines* have been developed to apply to situations where permanent video surveillance cameras have been placed on school property. These *Guidelines* are not intended to deal with instances where school officials videotape a specific event (such as a school fun fair, or graduation ceremony), or an isolated instance where a classroom is videotaped for educational or research purposes (for example, where a student teacher is required to record his or her lesson as part of an assignment for a work placement).

It is also important to note that the *Guidelines* do not apply to "covert surveillance." Covert surveillance refers to surveillance conducted by means of hidden devices, without notice to the individuals being monitored.[2]

However, the *Guidelines* will apply in any instances where a school board has set up permanent cameras to monitor students, including instances where cameras are used in school buses. Where school boards have entered into agreements with service providers to provide bussing, boards should take steps to ensure that the practices of service providers also adhere to the *Guidelines*. This requirement is dealt with at greater depth on page 7.

[2] The subject of covert surveillance is briefly addressed in Appendix A.

Definitions

In these *Guidelines*:

Institution is defined in section 2 of the municipal *Act* by way of a list of public bodies that are deemed to be institutions and are therefore subject to the *Act*. "School Boards" are included in the definition. Section 2 of the provincial *Act* states that an "institution" refers to any ministry of the government of Ontario. Therefore, both public and separate school boards, as well as provincial schools, are subject to the *Acts*.

Personal Information is defined in section 2 of the *Acts* as being recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex and age. Therefore a simple image on a video surveillance system that is clear enough to identify a person, or the activities in which he or she is engaged in, will be classified as "personal information" under the *Acts*.

Record is defined in section 2 of the *Acts* to mean any information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record and any record that is capable of being produced from a machine-readable record.

Video Surveillance System refers to a video, physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of individuals in school buildings and on school premises. In these *Guidelines*, the term video surveillance system includes an audio device, thermal imaging technology or any other component associated with recording the image of an individual.

Policy refers to the written document drafted by school board officials that codifies institutional obligations with respect to the collection, use, disclosure, retention and disposal of personal information.

Procedures refers to a written document that elaborates upon the school's duties with respect to the day-to-day operations of the surveillance system. These procedures are adopted at the board level. A board's written procedures will also address the collection, use, disclosure, retention, disposal and access to information as necessary.

Reception Equipment refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

Storage Device refers to a videotape, computer disk or drive, CD-ROM, computer chip, or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.

Collection of Personal Information Using Video Surveillance

Any recorded data or visual, audio or other images of an identifiable individual falls within the definition of "personal information" under the *Acts*.

Since video surveillance systems in schools would normally be set up to collect personal information about identifiable individuals, school boards must determine if they have the authority to collect personal information in accordance with the *Acts*.

Section 28(2) of the municipal *Act* (section 38(2) of the provincial *Act*) states that no person shall collect personal information on behalf of an institution (including school boards) unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

In order to justify any proposed or existing video surveillance system, a school board must be able to demonstrate that any collection of personal information will be authorized under one of these provisions under the *Acts*.

How to Decide Whether to Use a Video Surveillance System

Before deciding to use video surveillance, it is recommended a school board consider the following:

- Video surveillance should only be considered where less intrusive means of deterrence, such as increased monitoring by teachers, have been shown to be ineffective or unworkable. In its consultation with the school community, the board should outline the less intrusive means that have been considered and the reason why they are not effective.
- Before implementing a video surveillance program, a school should be able to demonstrate:
    - a history of incidents occurring in the specific school; and
    - the physical circumstances of the school – does it permit ready access to unauthorized individuals; is there a history of intrusion by unauthorized individuals; are there specific safety issues involving that school; and
    - whether a video surveillance program would be effective in dealing with or preventing future incidents of the type that have already occurred.
- Video surveillance programs should only be adopted where circumstances have shown that it is necessary for the purposes of enhancing the safety of students and staff, or for the deterrence of destructive acts, such as vandalism.
- The board should provide justification for the use and extent of a video surveillance program on the basis of enhancing safety and deterring destructive acts.
- The board should conduct an assessment into the effects that the surveillance system will have on personal privacy and the ways in which such adverse effects may be mitigated.
- The board should consult openly with parents, staff, students and the broader school community as to the necessity of the proposed video surveillance program and its acceptability to the school community. Consultation should provide stakeholders with an opportunity to comment on the actual location of cameras on school property, should the project proceed.
- The board should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required lawful goals.

Developing the Board Policy for Video Surveillance

Where a decision has been made by a school board to use a video surveillance system, the board should develop and implement a written **policy** regarding its operation. Where a board prefers to have a brief policy, some of these procedural elements may be addressed in the board's procedures (see pages 11–12 of these *Guidelines*). This policy should include:

- The rationale, objectives and justification for implementing the video surveillance program.
- A reference to the design requirements for every school where the video cameras are located. These requirements should refer to the fact that cameras should only be installed in places where surveillance is deemed necessary. The policy should also make reference to which personnel will be authorized to operate the system.
- Permitted locations for video cameras. While the policy may broadly set out the locations in schools where video surveillance is prohibited, all camera locations should ultimately be authorized by the school board.
- The policy should contain a statement outlining the times when the video surveillance will take place. Boards should consider the use of cameras activated by motion detectors to minimize the amount of time surveillance will be in place.
- The school board's obligations under the *Acts* with respect to notice, access, use, disclosure, retention, security and disposal of records containing personal information. (See pages 11–13.)
- The designation of a senior board staff member to be responsible for the board's privacy obligations under the *Acts* and its policy. This individual should also be responsible for advising staff at each school of the need to comply with the *Acts*.
- Board employees and service providers will have access to the personal information collected under the program *only* where necessary in the performance of their duties and where the access is necessary and proper in the discharge of the board's functions.
- The requirement that the board shall maintain control of, and responsibility for, the video surveillance system at all times.
- A requirement that any agreements between the board and service providers state that the records dealt with or created while delivering a video surveillance program are under the board's control and are subject to the *Acts*.

- A requirement that employees and service providers review and comply with the policy and the *Acts* in performing any duties and functions that are related to the operation of the video surveillance program. The policy should also state that employees will be subject to discipline for knowingly or deliberately breaching the policy or the provisions of the *Acts* or other relevant statutes. In cases where a service provider fails to comply with the policy or the provisions of the *Acts*, the policy should state that it will be considered to be breach of contract leading to penalties up to and including contract termination.

- Employees of service providers should sign written agreements regarding their duties under the policy and under the *Acts*, including an undertaking of confidentiality.

- A requirement that there is a process in place to appropriately respond to any inadvertent disclosures of personal information. The IPC paper, *What to do if a privacy breach occurs: Guidelines for government organizations*,[3] may be useful in this regard.

- The incorporation of the policy into the training and orientation programs of the board or the service provider. Training programs addressing staff obligations under the *Acts* should be conducted on a regular basis.

- The policy should be reviewed and updated regularly, at least once every three years.

[3] www.ipc.on.ca/docs/prbreach.pdf.

Designing, Installing and Maintaining Video Surveillance Equipment

In designing a video surveillance system and installing equipment, a school board should consider the following:

- Reception equipment such as video cameras, or audio or other devices should only be installed in identified areas where video surveillance is necessary and viable as a means of detection or deterrence of criminal or otherwise undesirable acts, or as an effective safety measure.

- The equipment should be installed in a way that it only monitors those spaces that have been identified as requiring video surveillance. Cameras should not be directed to look through the windows of adjacent buildings, or onto adjacent property.

- If cameras are adjustable by operators, this practice should be restricted, if possible, so that operators cannot adjust or manipulate the cameras to overlook spaces that are not intended to be covered by the video surveillance program.

- Video monitors should not be located in an area that allows for public viewing.

- Equipment should never monitor the inside of areas where students, staff and the public have a higher expectation of privacy (e.g., change rooms and washrooms).

- The board should consider the use of motion detectors to limit the time when the video surveillance cameras are in operation.

- Students, staff and the public should be notified, using clearly written signs, prominently displayed at the perimeter of the video surveillance area, of video surveillance equipment locations, so that each person has reasonable and adequate warning that surveillance is, or may be, in operation.

- Boards should adhere to the notification requirements under section 29(2) of the municipal *Act* (section 39(2) of the provincial *Act*). This provision requires that institutions inform individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used and the title, business address and telephone number of someone who can answer questions about the collection. At a minimum, there should be a sign in place that notifies individuals of the recording and informs them that they may contact the school office with any questions. The remainder of the notice requirements under the *Acts* can be satisfied through information pamphlets available in the school office.

- Boards should adhere to a strict maintenance program for video cameras, including image refocusing and lens cleaning. Service providers should visit schools three to four times per year to ensure that video cameras and recording equipment are operating properly, according to manufacturers' specifications. Any issues or concerns regarding the performance of such equipment should be followed up with immediately.

Procedures Governing the Use, Disclosure, Retention, Security and Disposal of Video Surveillance Records

Any information obtained through video surveillance systems may only be used for the purposes set out in the policy and must relate to the protection of students, staff and the public, including the discipline or consequences that arise from that, or it must assist in the detection and deterrence of criminal activity and vandalism. Information should not be retained or used for purposes other than those described in the policy.

Because video surveillance systems create a record by recording personal information, each board with a system should implement written **procedures**. The board is responsible for the content of the procedures, including the meeting of the minimum standards as set out below:

- Video surveillance should not be used for monitoring staff performance.
- All tapes or other storage devices that are not in use should be stored securely in a locked receptacle located in a controlled-access area. Each storage device that has been used should be dated and labelled with a unique, sequential number or other verifiable symbol.
- Access to the storage devices should be limited to authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material, to provide for a proper audit trail.

Boards should also ensure that procedures address the use and retention of recorded information such that they:

- Clearly state who can view the information and under what circumstances it may be viewed. For instance, the real-time viewing of the recorded information may be limited to the school principal and a designated alternate (such as the vice-principal). Circumstances that warrant a review should be limited to instances where an incident has been reported/observed or to investigate a potential crime.
- Provide that where real-time viewing of the monitors takes place, the authority to view the monitors may only be delegated by the principal to a limited number of individuals.
- Set out the retention period for information that has not been viewed for law enforcement, school or public safety purposes. Recorded information that has not been used in this fashion should be routinely erased according to a standard schedule. Normally, unused tapes should be erased on a schedule not exceeding one month. The relevant retention periods should be clearly documented in both the board policy and in the board's procedures.

- Establish a separate retention period when recorded information has been viewed for law enforcement, school or public safety purposes. Section 5 of Ontario Regulation 823 under the municipal *Act* (section 5(1) of Ontario Regulation 460 under the provincial *Act)* requires that personal information that has been used must be retained for one year. The length of this retention period may be reduced by way of a formal resolution by the school board.

- Require the school to store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them. A storage device release form, or an entry in a logbook, should be completed before any storage device is disclosed to the appropriate authorities. The form should indicate who took the device, under what authority, when this occurred and if it will be returned or destroyed after use. This activity should be regularly monitored and strictly enforced.

- Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include shredding, burning or magnetically erasing the personal information.

Access to Personal Information

Any student, staff member or member of the public that has been recorded by a video surveillance camera has a general right of access to his or her personal information under section 36 of the municipal *Act* (section 47 of the provincial *Act*). Policies and procedures must recognize this right. Access may be granted to one's own personal information in whole or in part, unless an exemption applies under section 38 of the municipal *Act* (section 49 of the provincial *Act*).

One exemption that may apply is contained in subsection 38(b) of the municipal *Act*, which grants the heads of institutions the discretionary power to refuse access where disclosure would constitute an unjustified invasion of another individual's privacy.

As such, access to an individual's own personal information in these circumstances may depend upon whether any exempt information can be reasonably severed from the record. One way in which this may be achieved is through digitally "blacking out" the images of other individuals whose images appear on the videotapes.

Auditing and Evaluating the Use of Video Surveillance

School boards should ensure that the use and security of video surveillance equipment is subject to regular audits. These audits should also address the institution's compliance with operational policies and procedures. An external body may be retained in order to perform the audit. Any deficiencies or concerns identified by the audit must be addressed as soon as possible.

Employees and service providers should be aware that their activities are subject to audit and that they may be called upon to justify their surveillance interest in any given individual.

The board should regularly review and evaluate its video surveillance program in order to ascertain whether it is still justified in accordance with the requirements listed on page 5. This should include an assessment of whether the deployment of cameras at a particular school remains justified. This evaluation should occur at least once every three years.

Other Resources

The personal information recorded by a school board's video surveillance system, and the board's policies and practices respecting the personal information, are subject to the privacy protection provisions of the *Acts*.

Prior to implementing a video surveillance system or, for that matter, any new program with privacy implications, school boards should seek legal advice and consult with their Freedom of Information and Protection of Privacy Co-ordinator.

The IPC monitors compliance with the privacy protection provisions of the *Acts*. If an institution intends to introduce, significantly modify or expand a video surveillance system, it should consult with the IPC.

Appendix A – Covert Surveillance

Covert surveillance occurs wherever surveillance cameras are set up without notification. Because covert surveillance takes place without notice to the public, individuals will not generally be aware that they are being monitored. As such, the practice of covert surveillance is one that has the potential of being highly privacy-invasive and should only be used as a last resort in limited case-specific circumstances. Prior to deciding to use covert surveillance, a school board should conduct a comprehensive assessment of the privacy impacts associated with the implementation of such a program. In all cases, where it takes place, covert surveillance should be time-limited.

The purpose of the assessment is to ensure that covert surveillance is the only available option under the circumstances and that the benefits derived from the personal information obtained far outweigh the violation of privacy of the individuals observed.

An example of a situation in which time-limited covert surveillance may be justified is where there is an ongoing problem of computer theft from the school's computer room. If other investigative techniques have been attempted, and have failed, the school may decide to install covert surveillance equipment in order to identify the thief. Such camera equipment should be positioned in a way that minimizes surveillance (i.e., the camera should be positioned so that individuals will only be recorded if they approach the computer equipment). After a suspect has been identified, the surveillance equipment should be removed.

A school board that uses covert surveillance as a case-specific investigation tool may consider developing, as part of sound privacy protection practices, a protocol that establishes how the decision to use covert surveillance is made on a case-by-case basis. The protocol should also include privacy protection practices for the operation of the system.

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca